(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 May 2012 (18.05.2012)

PCT

(10) International Publication Number
WO 2012/064263 A1

(51) International Patent Classification:
H04L 12/28 (2006.01) ***G08B 21/00*** (2006.01)
G07C 9/00 (2006.01) ***H04M 11/00*** (2006.01)
G08B 13/00 (2006.01) ***H04M 11/04*** (2006.01)

(21) International Application Number:
PCT/SE2011/051331

(22) International Filing Date:
8 November 2011 (08.11.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1051173-1 9 November 2010 (09.11.2010) SE
1051172-3 9 November 2010 (09.11.2010) SE

(71) Applicant *(for all designated States except US)*: **ZAPLOX AB** [SE/SE]; c/oBeta 5, Schelevägen 17, S-223 70 Lund (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **TILLY, Lars** [SE/SE]; Östra Ansgarigatan 53, S-216 13 Limhamn (SE). **GRIPWALL, Stefan** [SE/SE]; Wachtmeisters väg 20, S-252 84 Helsingborg (SE).

(74) Agent: **AWAPATENT AB**; Box 5117, S-200 71 Malmö (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) **Title**: METHOD AND SYSTEM FOR REMOTE OPERATION OF AN INSTALLATION

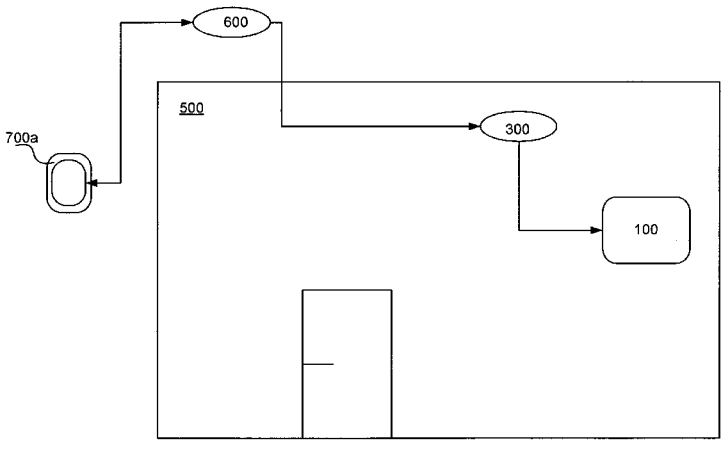

Fig. 1

(57) **Abstract**: The present invention relates to a method and a system for operating a device (100). The system comprises: a mobile communication device (700a), an internal server (300) and an external server (600), the external server (600) being adapted to generate a certificate and to send the certificate to the mobile communication device (700a),the mobile communication device (700a) being adapted to send a device specific command comprising the certificate to the internal server (300), the internal server (300) being adapted to check and validate the device specific command comprising the certificate, the internal server (300) being adapted to send a request to the device (100) to perform an action specified in the device specific command if the internal server (300) validates the device specific command comprising the certificate, the device (100) being adapted to perform the action, wherein the device specific command from the mobile communication device (700a) to the internal server (300) is adapted to be sent via a cellular network.

WO 2012/064263 A1

METHOD AND SYSTEM FOR REMOTE OPERATION OF AN INSTALLATION

Technical field

The present invention relates to a method and a system for operating a device.

Background art

Conventional keys provide a well established access control to properties like buildings and vehicles. A problem with such keys is that they are easily lost and/or copied causing costly lock bolt replacements. Furthermore, real estate agents, craftsmen, and home-help service staff are usually quite reluctant when it comes to handling (customers') keys. There is a need for keys that are both secure and easy to use.

Summary of the invention

In view of the above, an objective of the invention is to solve or at least reduce one or several of the drawbacks discussed above. Generally, the above objective is achieved by the attached independent patent claims.

According to a first aspect, the present invention is realized by a method for operating a device. The method comprises: an external server generating a certificate, the external server sending the certificate to a mobile communication device, the mobile communication device sending a device specific command to an internal server, wherein the device specific command comprises the certificate, the internal server checking the device specific command comprising the certificate, if the internal server validates the device specific command comprising the certificate: the internal server sending a request to the device to perform an action specified in the device specific command, the device performing the action, wherein the device specific command from the mobile communication device to the internal server is sent via a cellular network.

By a certificate is generally meant a digital authorization. For example, the certificate may be a digital authorization which authorizes a person to

operate a device. Further, in case the device is a door lock, the certificate may be thought of as a digital key.

By the method of the invention, it becomes easy and flexible to distribute certificates since the certificates are distributed in an electronic form to a mobile communication device from a server. Expressed differently, it becomes easy and flexible to authorize a person to operate a device, such as a door lock. Further, the method makes it easy for an authorized person to operate a device via a mobile communication device.

Further, the method is advantageous in that it is very secure since it operates via the cellular network. Furthermore, the method is advantageous in that a mobile communication device communicating via the cellular network is used for communication with the internal server, i.e. the mobile communication device need not be able to use WLAN, Bluetooth or other NFC (near field communication). The cellular network is advantageous in that it is robust, has a low uptime compared to ADSL and a high capacity, in that there is no wire to cut and difficult to tap. Moreover, if the mobile communication device is lost, the access for that specific mobile communication device is easily restricted which further increases the security. Furthermore, the method enables remote operating of the device.

The device specific commands sent by the mobile communication device to the internal server may be encrypted. Thereby the security is further increased.

Alternatively, instead of sending the certificate to the mobile communication device, the certificate is sent to a server. The server then forwards the certificate to a suitable party. This party could, e.g., be a mobile communication device.

The method may further comprise the mobile communication device signing the device specific command with a signing key before sending the device specific command to the internal server.

The method may further comprise: the external server generating the signing key, the external server sending the signing key to the mobile communication device, and the mobile communication device signing device specific commands using the signing key. This is advantageous in that the

signing provides information on from which mobile communication device the device specific command has been sent.

The signing key may identify the mobile communication device by which a device specific command has been signed.

The certificate may be associated with the signing key. The certificate may certify the authenticity of the signing key. The authenticity may be guaranteed by a certificate provider which is associated with the external server. The signing key could, e.g., be encrypted with a public key of the certificate provider.

The external server may use a digital identification when generating at least one from the group of the certificate and the signing key. This is advantageous in that the security is even more increased. The identification may, e.g., be information stored in a magnetic striped card used in conjunction with a card reader. Alternatively, the identification may be an electronic identification provided by, e.g., a bank. As a further alternative, the identification may be of analogue type, i.e., the identification is at least one one-time code provided on a piece of paper.

The certificate and the signing key may be limited in time. This is advantageous in that the flexibility and security is increased.

The method may further comprise the external server or the internal server revoking the certificate. This is advantageous in that the flexibility and security is further increased. By revoking a certificate, is meant that the certificate is invalidated. In other words, the certificate may no longer be used to authorize a person to operate a device. In this way, previously generated certificates may be revoked such that they may no longer be used by a person to operate a device.

The device specific command from the mobile communication device to the internal server may be sent via an external server via the cellular network, wherein if the external server validates the certificate, the external server sends the device specific command to the internal server via the cellular network. This is advantageous in that the system is made even more secure. The mobile communication device does not need to know the IP address of the internal server, only the IP address of the external server.

The request from the internal server to the device may be sent via a short range wireless protocol. This is advantageous in that wires do not disturb the aesthetic appearance and in that the installation is simplified.

The short range wireless protocol may be at least one from the group of Bluetooth, ZigBee, and WLAN.

The method may further comprise at least one of: the internal server storing information about which mobile communication device has been validated by the internal server, or the external server storing information about which mobile communication device has been validated by the internal server. The internal server storing the information is advantageous in that the privacy of the involved parties is protected. The external server storing the information is advantageous in that the information is backed-up.

The method may further comprise setting certificates via a web interface. This is advantageous in that flexibility and ease of use is provided. Furthermore, the user is provided with a good overview.

The device may be a lock module, the device specific command may be a lock/unlock command, and the step of the device performing the action may be the lock module locking/unlocking. This is advantageous in that a mobile communication device is easily authorized for locking/unlocking the lock module which means that, e.g., a craftsman and/or a real estate agent can easily be authorized through his/her mobile communication device. Furthermore, a craftsman can be granted access to a home during a limited period of time, e.g., Monday-Friday and/or during limited hours, e.g., 8 a.m. to 4 p.m.

The lock module may comprise a mechanical lock. This is advantageous in that a conventional key can also be used.

The method may further comprise the external server generating the certificate upon receiving an alarm event. This is advantageous in that a party may gain access to the device when something undesirable has happened that needs to be dealt with.

The method may further comprise the external server selecting a first party from a predetermined list, wherein the selecting comprises selecting a party which is geographically closest to the internal server using Global

Positioning System, and sending the certificate to the first party. This is advantageous in that the chances of reducing the damages caused by the undesirable event may be increased.

The method may further comprise the internal server generating an alarm event in case a sensor detects an undesirable event.

The sensor may be at least one from the group of a humidity detector, a liquid flow sensor, a smoke sensor, a fire detector, a capacitive sensor, and a crushing sensor.

The undesirable event may be at least one from the group of a fire, a leak, an overflow, and a housebreaking.

According to a second aspect, the present invention is realized by a system for operating a device. The system comprises: a mobile communication device, an internal server, and an external server, the external server being adapted to generate a certificate and to send the certificate to the mobile communication device, the mobile communication device being adapted to send a device specific command comprising a certificate to the internal server, the internal server being adapted to check and validate the device specific command comprising the certificate, the internal server being adapted to send a request to the device to perform an action specified in the device specific command if the internal server validates the device specific command comprising the certificate, the device being adapted to perform the action, wherein the device specific command from the mobile communication device to the internal server is adapted to be sent via a cellular network.

The advantages of the first aspect are equally applicable to the second aspect. Furthermore, the second aspect can be embodied in the corresponding embodiments of the first aspect.

Other objectives, features and advantages of the present invention will appear from the following detailed disclosure, from the attached claims as well as from the drawings.

Generally, all terms used in the claims are to be interpreted according to their ordinary meaning in the technical field, unless explicitly defined otherwise herein. All references to "a/an/the [element, device, component, means, step, etc]" are to be interpreted openly as referring to at least one

instance of said element, device, component, means, step, etc., unless explicitly stated otherwise. The steps of any method disclosed herein do not have to be performed in the exact order disclosed, unless explicitly stated.

Brief Description of the Drawings

Other features and advantages of the present invention will become apparent from the following detailed description of a presently preferred embodiment, with reference to the accompanying drawings, in which

Fig. 1 is schematic drawing of an embodiment of the inventive system.

Fig. 2 is schematic drawing of an embodiment of the inventive system.

Fig. 3 is schematic drawing of an embodiment of the inventive system.

Detailed description of preferred embodiments of the invention

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which certain embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided by way of example so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

Fig. 1 discloses an embodiment of the inventive system for operating a device 100. The system comprises a mobile communication device 700a, an external server 600, and an internal server 300. The mobile communication device 700a sends a device specific command comprising a certificate to the external server 600, via a cellular network. Before sending the device specific command, the mobile communication device 700a signs the device specific command using a signing key. The external server 600 checks the signed device specific command comprising the certificate. If the external server 600 validates the signed device specific command comprising the certificate, the external server 600 forwards the signed device specific command comprising a certificate to the internal server 300. The internal server 300 checks the

signed device specific command comprising the certificate. If the internal server 300 validates the signed device specific command comprising the certificate, the internal server 300 sends, via a short range wireless protocol, a request to the device 100 to perform an action specified in the signed device specific command. The device 100 then performs the action.

The certificate is generated by the external server 600 and sent to the mobile communication device 700a or, alternatively, to a server which can forward the certificate to the mobile communication device 700a. The mobile communication device can, e.g., be a mobile phone. The certificate is an authorization that authorizes the party to which the certificate is sent, e.g. the mobile communication device 700a, to send device specific commands to a certain device specified in the certificate.

In one embodiment, the certificate is generated in case an alarm event is generated.

The signing key identifies the mobile communication device by which a device specific command has been signed. More specifically, the signing key may comprise information regarding the identity of the mobile communications device by which a device specific command has been signed.

The certificate is associated with the signing key. The certificate certifies the authenticity of the signing key. The authenticity is guaranteed by a certificate provider which is associated with the external server 600. The signing key could, e.g., be encrypted with a public key of the certificate provider.

The certificate and/or the signing key may further be limited in time. For example, the certificate and/or the signing key may only be valid during business hours or during a specific day. In this way, the method and system may control when a user is allowed to operate a device by sending device specific commands.

The external server 600 may further revoke a certificate. As an effect of a certificate being revoked, a mobile communication device 700a that previously was authorized to send device specific commands is not allowed to

do so any longer. The external server 600 may thus end an authorization by revoking the corresponding certificate.

In one embodiment, the device 100 is a network camera. The network camera is arranged in a fridge. The device specific command is that the network camera is to send an image of the contents of the fridge to the mobile communication device. Thus, the user will then know if he/she ought to buy some milk on the way home. The device specific command may further be that the camera is to at least one of rotate, pan, tilt, zoom, adjust brightness. Since a certificate is necessary, the system is secure and only authorized parties may have access to the fridge.

The skilled person realizes that other types of devices are also possible. The device could, e.g., be a coffee maker and the device specific command could be that the coffee maker is to be turned off. Alternatively, the device can be a heating unit and the device specific command could be that the heating unit is to be turned on.

Fig. 2 discloses an embodiment in which the device is a lock module 800. The device specific command is a lock/unlock command. The device performing the action is the lock module 800 locking/unlocking. This embodiment enables that, instead of a mechanical key, a mobile communication device is used for locking/unlocking, e.g., a door. The information about which mobile communication devices have locked/unlocked a certain lock module can be stored in the internal server 300 and/or the external server 600. The information could also be presented in a web interface. In this way, it is possible to monitor, via the web interface, which mobile communication devices have locked/unlocked the lock module when. A parent can, e.g., see when the child is home again after school. A house owner is able to see when the cleaning firm or craftsman arrives and leaves.

In one embodiment, the system comprises at least one sensor 200. If the sensor 200 detects an undesirable event, the internal server 300 generates an alarm event. Then the internal server 300 sends a message to the external server 600 comprising information about which sensor has detected an undesirable event. The external server 600 generates a certificate and a signing key and sends the certificate and the signing key to a

predetermined server 900 which forwards the certificate and the signing key to the mobile communication device 700a. The mobile communication device 700a, or more particularly the person in possession of the mobile communication device 700a, is then able to enter the location 500 in which the undesirable event was detected by unlocking the lock module 800.

In the case wherein the sensor is a crushing sensor arranged at, e.g., a window and the undesirable event is a housebreaking, the device is preferably a lock module. Thus, a predetermined party, such as a security officer, is able to quickly enter the house.

As an alternative, the sensor is a smoke sensor and/or a fire detector. In case smoke and/or a fire is detected, a message is sent from the internal server to a fire department. Furthermore, a certificate and a signing key is generated by the external server and sent to the fire department so that the fire department easily can enter the location wherein the fire and/or smoke has been detected by unlocking the lock module, thus obviating the need to break down the door.

As a further alternative, the sensor is a capacitive sensor arranged in, e.g., a basement, an attic, or in the foundation of a building. The capacitive sensor may be arranged to detect undesired moist due to leaks caused by, e.g., rain, bad facade, and/or an inferior foundation.

Fig. 3 discloses yet an embodiment. An appliance 1000 (here a washing machine) using a liquid undesirably emits part or the liquid. The sensor 200 detects that the appliance 1000 has undesirably emitted part of the liquid. If the sensor 200 is a humidity detector, the detected level of humidity is sent to the internal server 300 via the short range wireless protocol. The internal server 300 compares the received level of humidity with a predetermined value and generates an alarm event if the received level of humidity is larger than a predetermined value. If the sensor 200 is a sensor arranged at an inlet of the appliance 1000, the sensor 200 detects how much liquid flows into the appliance 1000 per unit of time and sends the detected values to the internal server 300 via the short range protocol. The internal server 300 computes the amount of liquid that has flown into the appliance 1000 at a certain point of time using the information from the sensor 200. In

case the computed amount of liquid is larger than a predetermined value, the internal server 300 generates an alarm event. The internal server 300 sends a message to the external server 600 comprising information on that an alarm event has been generated and which appliance 1000 caused the alarm event to be generated.

In response to the alarm event, the external server 600 sends a certificate and a signing key to a predetermined first party 900. The predetermined first party 900 may, e.g., be a server at, e.g., a plumbing firm. The predetermined first party 900 forwards the certificate and the signing key to the mobile communication device 700a. The person having the mobile communication device 700a sees to that a signed unlock command is sent to the external server 600. The signed unlock command comprises the certificate. The external server 600 routes the signed unlock command to the correct internal server, in this case server 300. If the server 300 validates the certificate, the internal server 300 sends an unlock command to the lock module 800. The lock module 800 unlocks and the person holding the mobile communication device 700a can enter the location and hopefully reduce the damages caused by the emitted liquid.

In response to the alarm event, a message is sent to the owner of the appliance 1000, saying that appliance 1000 has caused an alarm event to be generated.

CLAIMS

1. Method for operating a device comprising:

an external server generating a certificate,

the external server sending the certificate to a mobile communication device,

the mobile communication device sending a device specific command to an internal server, wherein the device specific command comprises the certificate,

the internal server checking the device specific command comprising the certificate,

if the internal server validates the device specific command comprising the certificate:

the internal server sending a request to the device to perform an action specified in the device specific command,

the device performing the action,

wherein the device specific command from the mobile communication device to the internal server is sent via a cellular network.

2. Method according to claim 1, further comprising the mobile communication device signing the device specific command with a signing key before sending the device specific command to the internal server.

3. Method according to claim 2, further comprising:

the external server generating the signing key,

the external server sending the signing key to the mobile communication device, and

the mobile communication device signing device specific commands using the signing key.

4. Method according to claim 3, wherein the external server uses a digital identification when generating at least one from the group of the certificate and the signing key.

5. Method according to any one of claims 2-4, wherein the signing key comprises information regarding the identity of the mobile communication device by which a device specific command has been signed.

6. Method according to any one of claims 2-5, wherein the certificate is associated with the signing key, and wherein the certificate certifies the authenticity of the signing key.

7. Method according to any one of claims 2-6, wherein the certificate and/or the signing key are limited in time.

8. Method according to any one of the preceding claims, further comprising:

the external server or the internal server revoking the certificate.

9. Method according to any one of the preceding claims, wherein the device specific command from the mobile communication device to the internal server is sent via the external server via the cellular network,

wherein if the external server validates the certificate, the external server sends the device specific command to the internal server via the cellular network.

10. Method according to any of the preceding claims, wherein the request from the internal server to the device is sent via a short range wireless protocol.

11. Method according to claim 10, wherein the short range wireless protocol is at least one from the group of Bluetooth, ZigBee, and WLAN.

12. Method according to any one of the preceding claims, further comprising at least one of:

the internal server storing information about which mobile communication device has been validated by the internal server, or

the external server storing information about which mobile communication device has been validated by the internal server.

13. Method according to any one of the preceding claims, further comprising setting certificates via a web interface.

14. Method according to any one of the preceding claims,

wherein the device is a lock module,

wherein the device specific command is a lock/unlock command, and

wherein the step of the device performing the action is the lock module locking/unlocking.

15. Method according to any one of the preceding claims, further comprising the external server generating the certificate upon receiving an alarm event.

16. Method according to claim 15, further comprising the external server selecting a first party from a predetermined list, wherein the selecting comprises selecting a party which is geographically closest to the internal server using Global Positioning System, and

sending the certificate to the first party.

17. Method according to any one of claims 15-16, further comprising the internal server generating an alarm event in case a sensor detects an undesirable event.

18. Method according to claim 17, wherein the sensor is at least one from the group of a humidity detector, a liquid flow sensor, a smoke sensor, a fire detector, a capacitive sensor, and a crushing sensor.

19. Method according to any one of claims 17-18, wherein the undesirable event is at least one from the group of a fire, a leak, an overflow, and a housebreaking.

20. System for operating a device (100) comprising:

a mobile communication device (700a), an internal server (300), and an external server (600),

the external server (600) being adapted to generate a certificate and to send the certificate to the mobile communication device (700a),

the mobile communication device (700a) being adapted to send a device specific command comprising the certificate to the internal server (300),

the internal server (300) being adapted to check and validate the device specific command comprising the certificate,

the internal server (300) being adapted to send a request to the device (100) to perform an action specified in the device specific command if the internal server (300) validates the device specific command comprising the certificate,

the device (100) being adapted to perform the action,

wherein the device specific command from the mobile communication device (700a) to the internal server (300) is adapted to be sent via a cellular network.

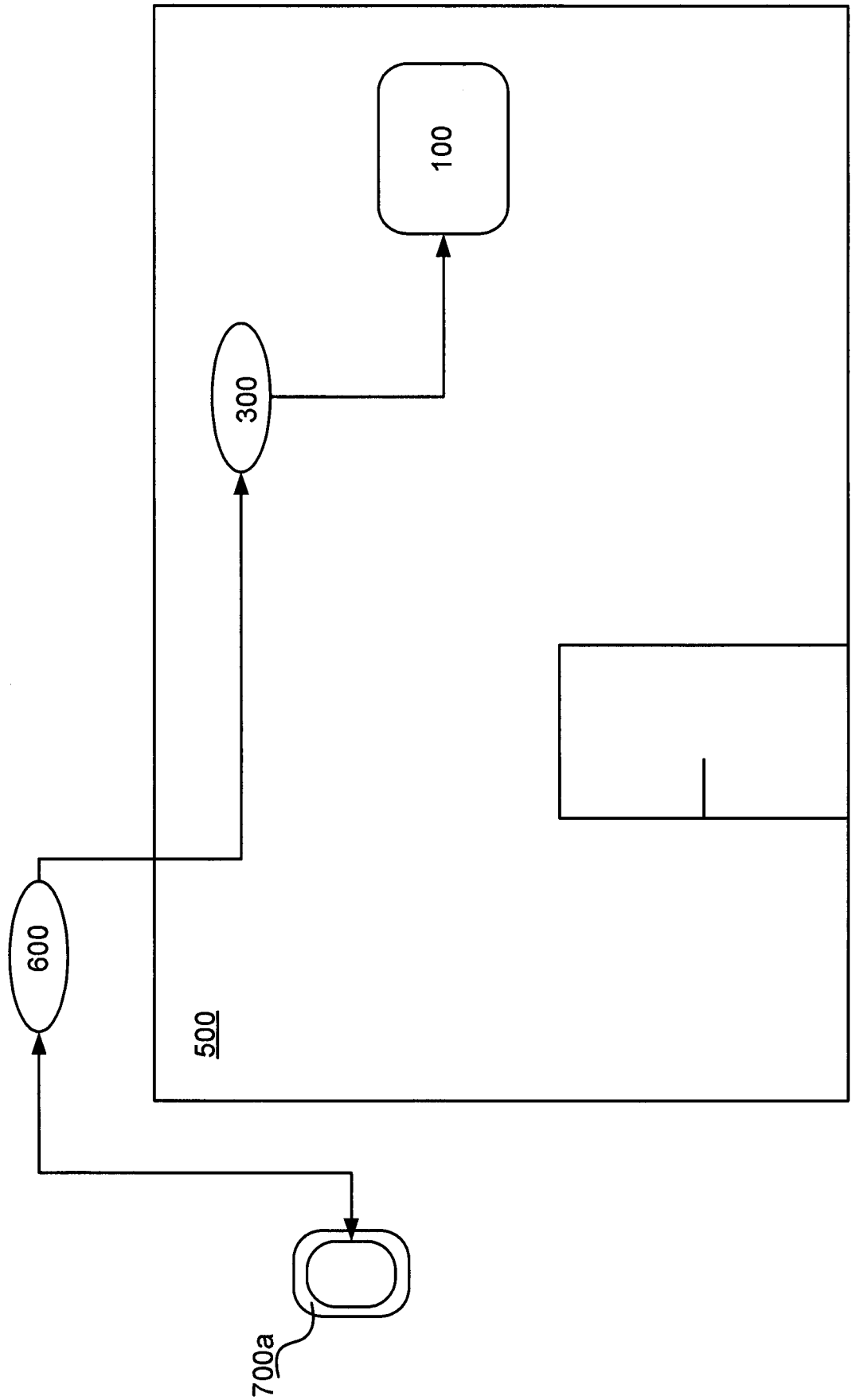

Fig. 1

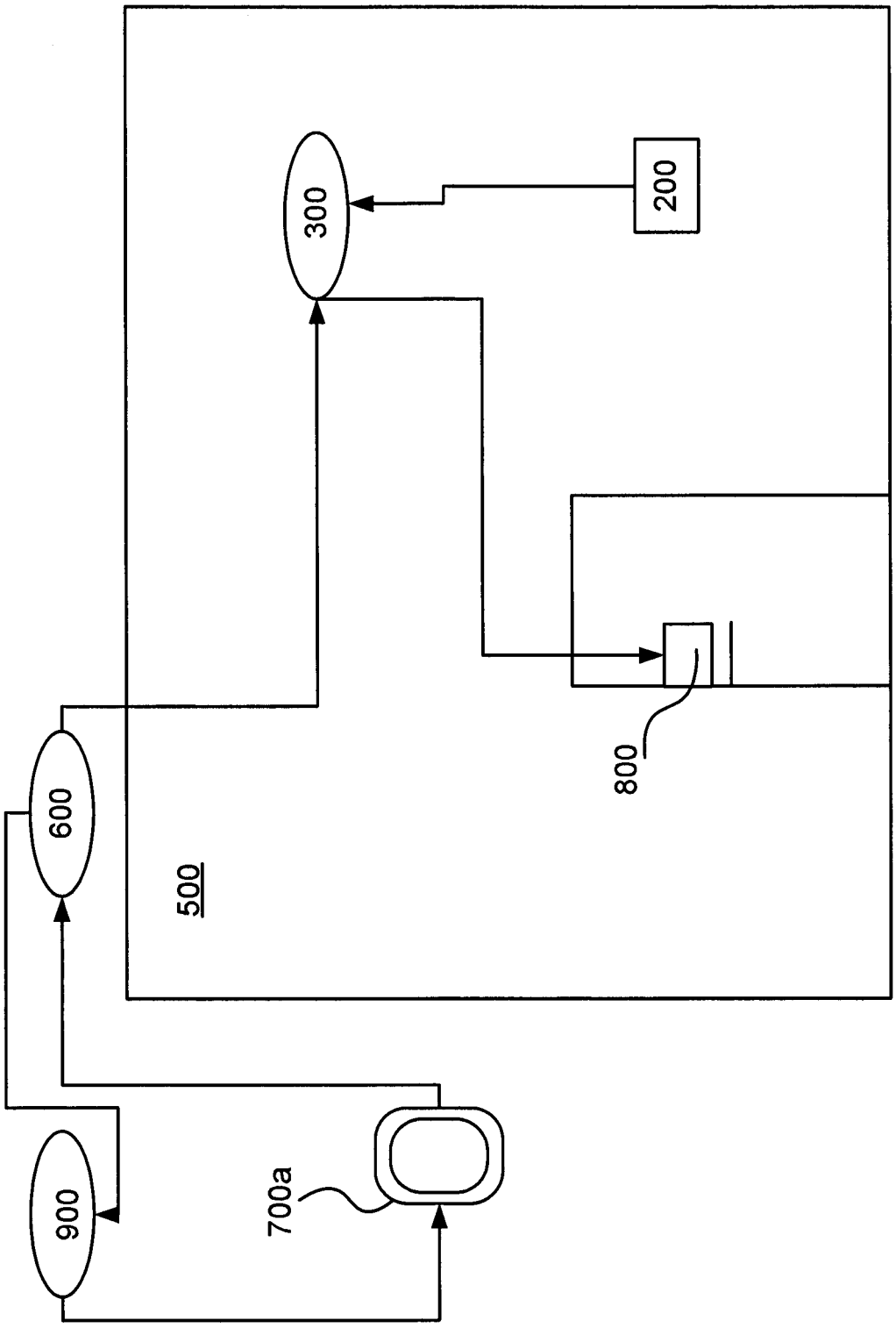

Fig. 2

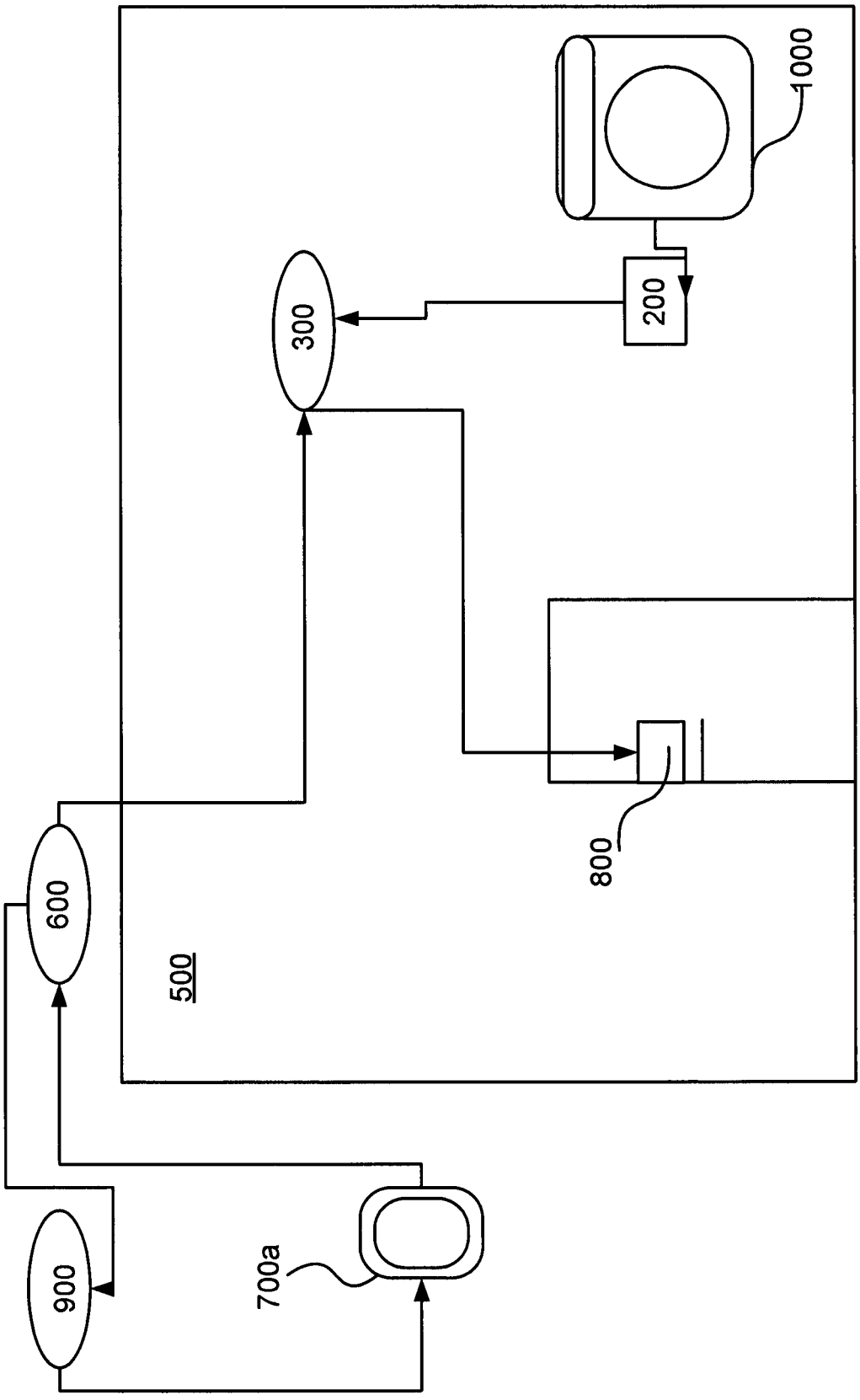

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2011/051331

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G07C, G08B, H04L, H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE, DK, FI, NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, PAJ, WPI data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2005080720 A1 (TAGMASTER AB ET AL), 1 September 2005 (2005-09-01); abstract; page 3, line 1 - page 3, line 31; page 6, line 30 - page 7, line 7; page 7, line 31 - page 8, line 5; figure 1; claims 1, 8 --	1-20
A	US 20070289012 A1 (BAIRD LEEMON), 13 December 2007 (2007-12-13); abstract; paragraphs [0012]-[0018]; figures 1-5; claims 1, 3 --	1-20
A	US 20060022816 A1 (YUKAWA MITSUHIKO), 2 February 2006 (2006-02-02); abstract; paragraphs [0002]-[0014], [0077]-[0087], [0094]-[0102]; figures 1,3,4,6,8 --	1-20

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08-03-2012	09-03-2012
Name and mailing address of the ISA/SE Patent- och registreringsverket Box 5055 S-102 42 STOCKHOLM Facsimile No. + 46 8 666 02 86	Authorized officer Per Karlsson Telephone No. + 46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2011/051331

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 20100138911 A1 (LIN CHUN-CHENG ET AL), 3 June 2010 (2010-06-03); abstract; paragraphs [0014]-[0018], [0025]-[0027], [0032], [0036]	1-20
	--	
A	US 20060250578 A1 (POHL GARRICK G ET AL), 9 November 2006 (2006-11-09); paragraphs [0003], [0023], [0094]-[0103]	1-20
	--	
A	WO 2009088901 A1 (SCHLAGE LOCK CO ET AL), 16 July 2009 (2009-07-16); abstract; paragraphs [0076], [0080], [0098]-[0090], [0099]-[0100]	1-20
	--	

Continuation of: second sheet

International Patent Classification (IPC)

H04L 12/28 (2006.01)
G07C 9/00 (2006.01)
G08B 13/00 (2006.01)
G08B 21/00 (2006.01)
H04M 11/00 (2006.01)
H04M 11/04 (2006.01)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/SE2011/051331

WO	2005080720	A1	01/09/2005	CN	1946912	A	11/04/2007
				CN	100588814	C	10/02/2010
				EP	1718826	A1	08/11/2006
				JP	2007523283	A	16/08/2007
				JP	4524306	B2	18/08/2010
				SE	525104	C2	30/11/2004
				SE	0400425	A	30/11/2004
				US	20080211620	A1	04/09/2008
US	20070289012	A1	13/12/2007	NONE			
US	20060022816	A1	02/02/2006	JP	2006048174	A	16/02/2006
US	20100138911	A1	03/06/2010	NONE			
US	20060250578	A1	09/11/2006	NONE			
WO	2009088901	A1	16/07/2009	AT	523002	T	15/09/2011
				AU	2008347260	A1	16/07/2009
				AU	2008347261	A1	16/07/2009
				CA	2711230	A1	16/07/2009
				CA	2711235	A1	16/07/2009
				EP	2235886	A1	06/10/2010
				EP	2232779	A2	29/09/2010
				US	20100283579	A1	11/11/2010
				US	20100318685	A1	16/12/2010
				WO	2009088902	A3	03/09/2009